AI USE BOUNDARY CHECK CARD

企业 AI 使用边界检查卡

在把真实资料、任务或客户信息带入 AI 工具前，先由业务负责人和参与岗位确认这 8 项。

适用对象：业务负责人、团队管理者、HR / 学习发展、内部推动者

这份资料用于帮助企业内部先对齐问题与优先级，不构成技术、法律或合规建议。

使用方式

选择一个准备尝试的任务，一项项确认。任何一项说不清楚时，先暂停输入真实资料，找负责人、IT 或合规伙伴澄清后再继续。

检查项	开始前要确认的问题	确认
任务目的	是否能说清楚这次使用 AI 要完成什么任务，而不是笼统地“提高效率”？	□ 已确认 □ 待澄清
业务负责人	是否有一位对任务结果负责的人，能决定什么可以尝试、什么必须停止？	□ 已确认 □ 待澄清
允许工具	是否确认所使用的工具、账号、版本和访问方式已获得组织许可？	□ 已确认 □ 待澄清
资料最小化	是否只带入完成任务所必需的内容，并优先使用脱敏、样例或公开资料？	□ 已确认 □ 待澄清
敏感信息	是否识别出客户资料、个人信息、报价、合同、代码或内部策略等不应随意输入的内容？	□ 已确认 □ 待澄清
权限与共享	是否知道谁能看到输入、输出和附件，是否需要额外授权？	□ 已确认 □ 待澄清
人工复核	是否明确哪些内容必须由人检查、确认或最终签发，不能直接对外使用？	□ 已确认 □ 待澄清
记录与异常	是否约定保留什么试用记录；发现错误、泄露疑虑或异常输出时找谁处理？	□ 已确认 □ 待澄清

试点中持续做的 4 件事

明确责任	让业务负责人、实际使用者和支持角色知道各自该决定什么、复核什么。
记录边界	记录这次试点允许用什么资料、工具和模板，避免口头理解不一致。
观察结果	同时观察效率、质量、误用风险和团队是否真的愿意复用。
处理变化	工具、资料或任务发生变化时，重新确认边界，而不是沿用旧判断。

提示：这是一份内部工作检查卡，不替代适用于您所在行业、地区或合同义务的法律、信息安全与合规判断。